DATA SECURITY and CONFIDENTIALITY HANDBOOK for NATIONAL MARINE FISHERIES SERVICE SOUTHEAST REGION

September, 1994

A. PURPOSE

1. The purpose of this handbook is to promulgate instructions dealing with operational responsibilities and procedures related to the collection, handling, maintenance, and release of confidential information defined in NOAA Directive NOA 216-100 Protection of Confidential Fisheries Statistics. Supplementary instructions will be issued as Annexes or as replacement pages to this manual from time to time.

2. The promulgation of data security regulations are an essential element in the protection of individual rights and trade secrets. Such regulations should not be construed as reflecting in any way on the honesty or integrity of any person, whether that person is authorized access to confidential data or not.

B. SCOPE

1. The operational responsibilities and procedures contained in this Handbook apply to all administrative and statutory confidential data, in any form and from any source, received or released by any employee of NMFS Southeast Region or by any authorized agent thereof.

2. "Confidential", as defined in NOAA Directive, NOA 216-100, is similar to "Controlled Information", as defined in the Department of Commerce Handbook of Security Regulations and Procedures (DOA 207-2). The DOC handbook does not specifically address the need for security procedures required by NMFS. This Handbook incorporates the policies from the DOC Handbook as they apply to "Controlled Information" and further develops those policies into a set of operating responsibilities and procedures for the types of data encountered by NMFS. Therefore, this Handbook constitutes the sole authority for handling such data.

3. This Handbook does not deal with the subjects listed below:

a. Physical protection of ADP equipment, facilities, data files and supporting utilities.
b. Protection of data communicated between and among computer Centers and remote terminal locations.
c. Hardware and software safeguards.

The above subjects are contained in the Department of Commerce ADP Security Manual. Responsibility for these matters rests with the manager of each ADP facility, with assistance from the appointed local ADP security officer.

C. RESPONSIBILITIES

1. Individuals.

Security is principally an individual responsibility. No amount of regulations can insure security without individual cooperation. All penalties for breaches of security are directed against the individual. A thorough knowledge of security regulations and constant individual vigilance are the best guarantees of security.

2. Program Administrators and Managers.

Supervisors and managers of programs or offices are individually responsible for the safeguarding of confidential data entrusted to them, and also responsible to ensure that persons under their supervision are aware of, and conform to, regulatory requirements dealing with confidential data.

3. Regional Data Base Administrator (RDBA).

The Regional National Marine Fisheries Service RDBA is individually responsible for safeguarding of confidential data entrusted to him/her, is responsible as a supervisor and manager, and is the principal individual in the Southeast Region with responsibility for establishing and enforcing mechanisms to safeguard all confidential data handled by any employee of the NMFS Southeast Regional or by any contractual or other agent thereof. RDBA's are guided by FIPS Pub 31 in the development of such mechanisms.

4. Comments and Suggestions.

All comments and suggestions dealing with the subject of data security within the scope of this Handbook should be communicated directly to the NMFS Southeast RDBA.

D. PROCEDURES

1. Access.

a. Access to confidential data will be restricted to those persons who require it in connection with the conduct of official Federal government fisheries-related business. Access is never granted to an office or other organization or group. Persons who require access may be Federal employees or any other person engaged in official Federal government fisheries-related business, including contractors and grantees.

b. Within the general rules stated above, access to confidential data under the purview of the NMFS Southeast Central Registry of Personnel Authorized Access to Confidential Data (the "Central Registry") will be granted only to persons whose names currently appear on the Central Registry of Personnel Authorized Access. The Central Registry is maintained by the NMFS Southeast RDBA.

c. The Central Registry contains the names and other data pertaining to persons who handle confidential data and whose need-to-know has been established, and who signed the "Standard Statement of Nondisclosure" (see Appendix C: NOA 216-100). The Central Registry is controlled as a confidential document. Information contained in it may be revealed only to authorized users as defined in NOAA Directive NOA 216-100.

d. The Central Registry will be consulted by authorized persons whenever it becomes necessary to convey confidential data to a person whose need-to-know is unknown. Authorized persons may consult the Central Registry by contacting the office of the NMFS Southeast RDBA in person or by telephone.

e. Each authorized user will be issued a unique Access Number at the time of completion of the Statement of Nondisclosure. This Access Number will be confidential, and will be used as identification when making telephone inquiries to the office of the RDBA. The Access Number will not be revealed to others, including other authorized users, outside the office of the RDBA.

f. Specific guidance pertaining to the handling of requests for confidential data, and to special procedures that apply to cold storage summary reports and to the release of administrative confidential data is contained in NOAA Directive NOA 216-100 (.04d through 3c.).

2. Collection.

a. Guidance concerning the collection of confidential data is contained in, NOA 216-100, (Section 6. Procedures, .01 Data Collection.)

b. The names of all collectors of data will be recorded in the Central Registry in accordance with paragraph D. 1. b. of this Handbook.

c. The same Statement of Nondisclosure will be signed by all collectors and other requiring access to administrative or statutory confidential data.

3. Maintenance (Safeguarding)

a. Definitions. For purposes of discussing the maintenance (or safeguarding) of confidential data, the following terms are used:

1). Manual Document: Any storage medium on which is recorded alphabetic, numeric and/or special characters in a form in which such characters may be read by the human eye. Examples of manual documents are (1) printed forms or notebooks with handwritten or typed entries, (2) punched cards and punched pater tape (whether interpreted or not), (3) graphs, maps, charts, tables and listings (whether prepared by hand, typewritten, word processor, computer or other device), and (4) any photographic or other reproduction, facsimile or extract thereof.

2). Non-Manual Document: Any storage medium that contains data in a form such that the characters or character representations cannot be read by the human eye. Examples are magnetic and other electronic storage media for data that are in digital form.

b. Safeguarding of Manual Documents.

1). Marking. Manual documents will be conspicuously marked with the words, "FISHERIES CONFIDENTIAL (ADM)" or "FISHERIES CONFIDENTIAL (STAT)" as soon as administrative or statutory confidential data are recorded on them. Whenever practicable, the marking will be in letters not less than one-half inch in height, and will be placed at the top and bottom center of every page, in red ink. The letters must be at least as large as any other characters or symbols

appearing on the page in all cases. Small documents that are handled in large numbers (such as punched cards and printed forms) may be placed in appropriate containers that have covers, flaps or lids, and the protective marking may be placed conspicuously on the outside of the container. Protective markings, rubber stamps on which they are embossed, and documents on which they appear will be protected from viewing by unauthorized persons. Documents containing both confidential and non-confidential data will bear the protective marking of the most sensitive data on each page.

2). **Shipping and Mailing.** Confidential data may be shipped or mailed by any conventional medium. Ordinary mail, Parcel Post, Air Express, United Parcel Service and similar media are all acceptable. Couriers who are not authorized access to the material may be used, as long as the materials are securely sealed in such a manner as to make undiscovered tampering unlikely. All confidential data will be double-wrapped or double-enveloped, with the full address of the recipient on both the inner and outer wrapping or envelope. The inner wrapping or envelope will be clearly marked in red ink with the protective marking. The protective marking will not appear on the outside of the package, nor will it be visible through the outer wrapper or envelope. These procedures apply to interoffice delivery of confidential data. A common security violation is for authorized users to carry confidential data through the hallways with the protective marking exposed. The proper security precaution is to place it in an envelope or fold it in such a way that the marking is not seen by others.

3). **Reproduction.** Copies of documents containing confidential data should be kept to the minimum number that are required for efficient operations. As a general rule, only the originator of a document should be permitted to make a copy or copies of it in whole or in part. The only exception to this is when it is clearly impractical, as in the case where data are incorporated into a digital file. Special written arrangements concerning reproduction will be made when manual documents are provided to persons outside NMFS.

4). **Storage.** Confidential data will be protected continuously from unauthorized knowledge, viewing or access. A common breach of security is to fail to cover confidential data when an unauthorized person enters the room. This can be accomplished in an unobtrusive manner so as not to bring embarrassment to the visitor. Another common error is to discuss confidential matters in public areas or over the telephone within possible hearing distance of unauthorized persons. When confidential documents are not in use, they will be placed in a heavy, locked container (file cabinet, locker, safe or desk) and secured by locking the container. Such documents should never be allowed to remain on a desk top or in any other unsecured location unguarded for any length of time. The lock may be of the built-in key type, or may be a padlock or a 3-position, dial-type combination lock. Confidential documents must not be stored in the same drawer with documents that do not contain confidential data. Under no circumstances will confidential documents be stored in any container to which unauthorized persons have access.

5). **Disposition/Destruction.** Confidential data are exempt from automatic decontrol. That is, there is no prescribed period of years beyond which FISHERIES CONFIDENTIAL data are released to the general public or to other persons who are not registered as authorized users at that future time. Confidential data that are no longer needed will be destroyed by any appropriate means that will insure their confidentiality. burning or shredding will be used when practicable. Documents containing confidential data on one side will not be recycled as scratch pads or for other uses. Documents bearing protective markings should never be placed in trash receptacles for routine disposal. As a minimum, protective markings should be removed and disposed of separately.

6). **Log Books.** A record or log will be maintained in each operating area where confidential data are received or dispatched. The log will contain a descriptive title of each confidential document received or dispatched, the date and time of the action, the number of pages or individual items involved, and the number of copies. The log will also show from whom each document was received or to whom it was dispatched. Logs will be filed in a secure place in a manner similar to that used for confidential data.

b. **Safeguarding of Non-Manual Documents.**

1). The physical safeguarding rules for storage devices bearing digital images or analog representations of confidential data (such as magnetic tapes, discs, floppy discs, cartridges and magnetic cards) are the same as those enumerated in paragraph 2., above.

2). Procedures for controlling access to, and safeguarding of, confidential data while the data are stored on the aforementioned devices as covered in the DOC, ADP Security Manual.

Implementation of such procedures is the responsibility of each ADP facility manager, with the assistance of the local ADP Security Officer.

E. PENALTIES - NOAA Directive, NOA 216-100 - Section 7 (July, 1994)

.01 Civil and Criminal. Persons who make unauthorized disclosure of confidential data may be subject to civil penalties or criminal prosecution under:

- **a.** Trade Secrets Act (18 U.S.C. 1905);
- **b.** Privacy Act (5 U.S.C. 552a (i) (1));
- **c.** Magnuson Act (16 U.S.C. 1858);
- **d.** MMPA (16 U.S.C. 1375)

.02 Conflict of Interest. Employees are prohibited by Department of Commerce employee conduct regulations [15 CFR part 0] and by ethics regulations applicable to the Executive Branch [5 CFR 2635.703] from using nonpublic information subject to the Order of personal gain, whether or not there is a disclosure to a third party.

.03 Disciplinary Action. Persons may be subject to disciplinary action, including removal, for failure to comply with this order. Prohibited activities include, but are not limited to, unlawful disclosure or use of the data, and failure to comply with implementing regulations or statutory prohibitions relating to the collection, maintenance, use, and disclosure of data covered by the Order.

RESPONSIBLE ORGANIZATION:

NATIONAL MARINE FISHERIES SERVICE
SOUTHEAST FISHERIES SCIENCE CENTER
SOUTHEAST REGIONAL
DATABASE ADMINISTRATOR
75 VIRGINIA BEACH DRIVE
MIAMI, FLORIDA 33149
PHONE: 305-361-4271